PURPOSE

To establish risk assessment and vulnerability management requirements and processes applicable to the Michigan Department of Health and Human Services (MDHHS) information systems.

REVISION HISTORY

Issued: 6/01/2021.
Next Review: 6/01/2022.

DEFINITIONS

Authorizing Official

A senior official or executive with the authority to authorize (for example, assume responsibility for) the operation of an information system or the use of a designated set of common controls at an acceptable level of risk to agency operations.

Authorization to Operate (ATO)

The official management decision given by a senior official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations.

Confidential Information

Sensitive information wherein unauthorized disclosure could cause serious financial, legal or reputational damage to an agency or the State of Michigan (SOM.) Confidential data may include personally identifiable information (PII) or confidential non-public information that relates to an Agency's business.

Enterprise Vulnerability Management (EVM) Program

The cyclical process of identifying, classifying and remediating vulnerabilities based on periodic scans of inventoried information systems in the network. The EVM Program is dependent on having a current and complete inventory of the information systems in the network. Without this information, vulnerable systems cannot be identified and remediated. The program does this by performing regular discovery scans to identify network assets.

Michigan Security Accreditation Process (MiSAP)

A risk management process which enables business and IT security stakeholders to evaluate the effectiveness of security controls and determine that residual risks are low enough to justify

issuance of the authority to operate (ATO) required before a system or capability moves from development into production -- or *go live*.

Personally Identifiable Information (PII)

Any information about an individual maintained by an agency with respect to, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information that can be used to distinguish or trace an individual's identity (such as name, Social Security Number, date and place of birth, mother's maiden name, biometric records) including any other personal information linked or linkable to an individual.

Workforce Member

Includes full and part-time employees, affiliates, associates, students, volunteers, contractors, and staff from third party entities.

POLICY

Timely risk assessments of MDHHS information systems are required to protect against potential threats and vulnerabilities that might otherwise compromise the confidentiality, integrity, and availability of sensitive and confidential information.

In compliance with Department of Technology, Management and Budget (DTMB) 1340.00, Information Technology Information Security Policy, MDHHS must ensure implementation of all moderate baseline security controls catalogued in the National Institute of Standards and Technology (NIST) Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations (Revision 4) from the NIST Computer Security Resource Center. This policy sets forth requirements from the risk assessment [RA] family of NIST controls managed by MDHHS in accordance with DTMB 1340.00.150.01, Risk Assessment Standard. MDHHS must review this policy annually.

Where applicable, this policy requires compliance with other federal and state laws, rules and regulations, policies, standards or other guidelines, including but not limited to the following:

- Centers for Medicare and Medicaid Services (CMS) Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges (MARS-E).
- Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Security Policy.

- Internal Revenue Service (IRS) Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies and Entities.
- Social Security Administration (SSA) Technical System Security Requirements (TSSR).
- U.S. Department of Health and Human Services Health Insurance Portability and Accountability Act (HIPAA), 45 CFR Part 160 and Part 164, Subparts A and C.

Security Categorization [RA-2]

MDHHS must:

- Categorize information and the information system in accordance with applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance.
- Document the security categorization results (including supporting rationale) in the system security plan for the information system.
- Ensure that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

Risk Assessment [RA-3]

MDHHS must:

- Conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.
- Document risk assessment results in the State of Michigan (SOM) Governance Risk and Compliance (GRC) tool.
- Review risk assessment results as part of the MiSAP at least annually or sooner when a significant change occurs, which include but are not limited to the following:
  - Changes in Information system owner, authorizing official, agency security, privacy officer or data custodian.

- Changes in the information system business scope, functions or system boundaries.
- Changes in information classification or system categorization.
- Changes in federal or state laws or regulatory compliance that impact the system.
- Changes in system architecture, such as hardware, software or firmware.
- Additions/deletions of system interconnections or information sharing.
- Changes in hosting locations or system support.
- Weakness or deficiencies discovered in currently deployed security controls.

- Disseminate risk assessment results to (responsible) DHHS staff assigned with business-side risk management for the information system as identified in the GRC tool, including but not limited to MDHHS Authorizing Official, Agency Security Officer, Agency Privacy Officer, or Data Custodian.

- Review the risk assessment as part of the MiSAP annually, and updates it once every three years or sooner when there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

Vulnerability Scanning [RA-5]

MDHHS must support DTMB implementation of the Enterprise Vulnerability Management (EVM) Program, in accordance with DTMB 1340.00.150.01, Risk Assessment Standard, by:

- Maintaining a current and complete inventory of the information systems in the network.
- Analyzing vulnerability scan reports and results from security control assessments.

- Remediating legitimate vulnerabilities in accordance with organizational assessments of risk; see tables in DTMB Standard 1340.00.150.01.
- Sharing information obtained from vulnerability scanning process and security control assessments with personnel identified as responsible staff through the GRC tool, within and throughout MDHHS, in coordination with DTMB, to help eliminate similar vulnerabilities in other information systems.

ROLES AND RESPONSIBILITIES

The MDHHS security officer and privacy officer must determine roles and responsibilities for Compliance and Data Governance Bureau personnel to support implementation of this policy.

MDHHS workforce members are responsible for reading, understanding, and complying with policies, standards, and procedures based on access controls.

ENFORCEMENT

Violations of this policy or failure to implement provisions of this policy may result in disciplinary action up to and including termination, civil litigation, and/or criminal prosecution.

REFERENCES

Federal Standards/Regulations:

NIST 800-53 rev.4:

RA-1 Risk Assessment Policy and Procedures
RA-2 Security Categorization
RA-3 Risk Assessment
RA-5 Vulnerability Scanning

45 CFR §164.306

45 CFR §164.306(a)(1) Security Categorization (R)

45 CFR §164.308

45 CFR §164.308(a)(1)(i) Security Management Process
45 CFR §164.308(a)(1)(ii)(A) Risk Analysis (R)
45 CFR §164.308(a)(1)(ii)(B) Risk Management (R)

45 CFR §164.308(a)(7)(ii)(E) Applications and Data Criticality Analysis (A)

45 CFR §164.316

45 CFR §164.316(a) Policies and Procedures

State Standards/Regulations:

MDHHS Policy Manuals

APL 68E-140 Applications and Data Criticality Analysis Policy and Procedure
APL 68E-340 Time Limit, Availability and Updates Policy
APO 531 Information Technology (IT) Data Classification

DMB Administrative Guide

DTMB IT Technical Policies, Standards and Procedures

1340.00.150.01 Risk Assessment Standard
1340.00.150.02 Data Classification Standard

CONTACT

For additional information concerning this policy, contact the MDHHS Compliance and Data Governance Bureau at MDHHSPrivacySecurity@michigan.gov.